TRACK MY PHOTO: EFFECTIVE TRACKING OF PHOTO SHARING IN SOCIAL MEDIA NETWORKS

KARTHIKA S¹, SOWMIYA D², SINDHUJA M³, PRASATH M⁴

¹, ³Assistant Professor, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamilnadu, India.
², ⁴Student, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamilnadu, India.
¹karthika@newprinceshribhavani.com
²sowmiyadoss11@gmail.com
³sindhuja@newprinceshribhavani.com
⁴m.prasathmurugesan@gmail.com

Abstract: Nowadays, continuous tracking of user photo in the social media networks is becoming important as people sharing many of their photos in social media. This system is very effective to track our photo sharing in social networks without our knowledge. In this project Matlab is used for face recognition concept. Every user has to register their faces in the main server which is considered for overall comparison & verification. Every user has to provide their credentials like Mobile number & Email ID for any notifications. Face book like social media is designed and user is allowed to share their photos to their friends. Once the user post a photo this server will immediately verify the Face recognition main server and Face recognition is initialized & verified using Matlab. If matched then alert notification is passed to the user, if the user allows / permits, then the photo is automatically posted in the face book like site, if not the photo sharing process is declined. This system is very much effective in such a way to prevent misuse of users’ photos and credentials and also server will act as intermediate layer in order to monitor users’ behavior. Both the user personal information like name, phone number, email id and photos will not be shared among themselves for the initial period of time. So server will monitor user behavior consistency. If server finds misbehavior in any time, user will be removed from the server. Apart from the above mentioned, friend suggestion based on likes and location is implemented.
Keywords: Privacy, Online Social Network, Flexibility, Feature Extraction

1. INTRODUCTION

An increasing number of people are using wireless mobile applications to share personal photos via online social networks (OSNs) such as Facebook. This has resulted in large quantities of photo collections in OSNs. To facilitate effective browsing, searching, categorization, and exportation (e.g., sending or printing) of photo collections, it is important to develop face annotation techniques that allow users to manage and organize personal photos in OSNs.

Collaborative FR framework consists of two major parts: selection of FR engines and merging (or fusion) of multiple FR results. In order to recognize query the images of face that belongs to a member of OSN, FR engines can be used. For this purpose, we exploit both social network context in an OSN and social context in personal photo collections.

Face recognition on a social network platform is differentiated from the previous web service in the way that the platform uses specialized social networks of people. The social network platform by itself is a new concept, which uses a social network service as the platform. Millions of users have integrated social network sites such as My space and Facebook into their daily practices to communicate with people who formed parts of the online social network. Photo images occupy a huge proportion of web contents and among them a large portion is face images. This shows that face recognition on a social network platform is becoming a new application.

2. RELATED WORK

A paper on “Moving beyond Untagging: Photo Privacy in Tagged World” by Andrew Besmer and Heather Richter Lipford [2] proposed a system in which “Restrict others” tool is used to address photo privacy. It works by allowing tagged users to send a request to the owner asking that a photo be hidden from certain people. The tagged user is able to set the custom permissions at the individual photo level. This tool promotes sharing by reducing the need for the tagged user to untag the photo or restrict all their tagged photos. This tool lets user specify individuals or
groups of users they would like to restrict the photo from. In [6], Your Privacy Protection works as a monitoring and recommender system. They have applied it to recommend privacy settings in a social network Facebook. In [7], classification models for specifically searching for private photos, and for diversifying query results to provide users with a better coverage of private and public content is proposed.

A paper on “Autotagging Facebook: Social Network Context Improves Photo Annotation” by Zak Stone, Todd Zickler, Trevor Darrell [8] proposed a framework in which task of automatic face recognition in personal photographs is done. Author combine face recognition scores with social context in a conditional random field (CRF) model and apply this model to label faces in photos from the popular online social network Facebook, which is now the top photo - sharing site on the Web with billions of photos in total. A conceptualization of privacy as the selective control of access to the self, involving dialectic, optimization, and multimodal processes is proposed in [1].

In 2009, Jonathan Anderson proposed a paradigm called Privacy Suites [4] which allows users to easily choose suites of privacy settings that can be created by an expert using privacy programming or can be created through exporting them to the abstract format or through existing configuration UIs.

In 2011, Barbara Carminati, Elena Ferrari , Raymond Heatherly, Murat Kantar-cioglub, Bhavani Thuraisingham [5], address that security and privacy concerns need to be addressed for creating applications of online social networks that include person specific information

3. EFFECTIVE PHOTO TRACING FRAMEWORK

A mechanism has been designed to make users aware of the posting activity and make them actively take part in the photo posting and decision making paradigm for which a facial recognition (FR) system is recommended which can recognize everyone present in the photo is explained in Figure 1. If more privacy setting is done then it may limit the number of photos which will be utilized as the training set for FR system. In order to overcome this problem and for training set for FR system we would utilize the private photos of users which would
differentiate the photo co-owners without affecting their privacy. A distributed consensus based method is developed which would protect the private training set and even reduce the computational complexity.

1. Register to become a member of the account.
2. Login to the application’s home page.
3. Enter OTP which will be sent to new user who desire to register.
4. Once registered, the user can upload images which then can be detected and cropped.
5. The user can search for their friends in their respective registered OSN if any or friend request can be sent.
6. If the registered user has received any friend request, it can be accepted.
7. The registered user will upload or add photo(s) in the home page.
8. The OTP has to be entered by the user which will be sent to the registered email ids of the users.
9. Face recognition algorithm is used to recognize the faces present in the uploaded photo.
10. If faces are recognized then notification is sent to the co-owner about posting activity.
11. Finally, if permission is given by the co-owner then photo will be uploaded.

Figure 1. Architecture of Photo Tracing

The proposed scheme is very useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade-off between privacy and utility. Preserving user privacy and making them actively participate in the photo posting activity is a very prime concern in OSNs. The co-photo can be posted only with the permission of the co-owner and if the privacy and exposure policy gets satisfies. To make the system more secured
the notification is sent to the co-owner and only with his/her acceptance the photo is posted. In addition random OTP is generated while uploading photo to verify the user who is posting it as someone may access his account to upload photos which are in actual not to be posted by the concerned account holder.

4. IMPLEMENTATION OF PHOTO TRACING

ALGORITHM FOR IMAGE PROCESSING
1. for number of scales in image uploaded do
2. down sample image by one scale
3. compute integral image for current scale
4. for each shift step of the sliding detection window do
5. for each stage in the cascade classifier do
6. for each filter in the stage do
7. Filter the detection window
8. end
9. Accumulate filter outputs within this stage
10. if accumulation fails to pass per-stage threshold do
11. break the for loop and reject this window as a face
12. end
13. end
14. if this detection window passes all per-stage thresholds do
15. accept this window as a face
16. else
17. reject this window as a face
18. end
19. end
20. end
4. PERFORMANCE EVALUATION

The result of the system is shown with the help of the comparison table where it shows the difference between the existing system and the system proposed. The result of the system depends on the number of images is shown in Figure 2 and 3. As the number of images increases the recognition of the owners and co-owners photo is done more easily and quickly.

![Recognition Ratio](image1)

**Figure.2 Recognition Ratio**

![Face Recognition Ratio](image2)

**Figure.3 Face Recognition Ratio**
5. CONCLUSION AND FUTURE WORK

The proposed framework is highlighted with low calculation expense and privacy of the preparation set. We expect that our proposed plan be exceptionally helpful in ensuring clients protection in photograph/picture sharing over online informal organizations. In our current android application the co-photo could only be posted with the permission of all the co-owners. Our future work could be how to move the proposed training schemes to personal clouds like Dropbox or iCloud.

REFERENCES


[8] Zak Stone, Todd Zickler, Trevor Darrell Auto tagging Facebook: Social Network Context Improves Photo Annotation.